příjmení: **MA – závěrečný test – varianta XV**

jméno: **4.2.2010**

skupina:

1. Určete, jaká x jsou řešeními soustavy kongruencí

$$3\,x \equiv 1 \pmod 4,$$
$$2\,x \equiv 1 \pmod 5,$$
$$2\,x \equiv 3 \pmod 9.$$

   Nezapomeňte soustavu nejprve transformovat na tvar odpovídající definici Čínské věty o zbytcích. [8 bodů]

2. Rekurzivní formulí, uvedenou na přednášce, spočtěte hodnoty čitatele a jmenovatele prvních čtyř sblížených zlomků k pravému řetězovému zlomku

$$x = [2; 3, 1, 4, 1, 5, 1, \dots].$$

   [8 bodů]

3. Tak zvaná *afinní šifra* je definována šifrovací transformací $\mathcal{C}(m) \equiv a \cdot m + b \pmod n$ a dešifrovací transformací $\mathcal{D}(c) \equiv a^{-1} \cdot (c - b) \pmod n$, přičemž musí existovat multiplikativní inverze a^{-1} a musí tedy platit, že $\gcd(a, n) = 1$. Zprávy šifrujeme a dešifrujeme po jednotlivých znacích.

   Přiřadíme-li jednotlivým znakům české abecedy ($n = 42$) jejich numerické ekvivalenty podle následující tabulky,

A	Á	B	C	Č	D	Ď	E	É	Ě	F	G	H	Ch	I	Í	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Ň	O	Ó	P	Q	R	Ř	S	Š	T	Ť	U	Ú	Ů	V	W	X	Y	Ý	Z	Ž
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41

   a zvolíme-li $a = 19$ a $b = 2$, obdržíme po zakódování textu šifrovanou zprávu ŘÉSŤA OQ ĎŤFTÉA, přičemž mezery se zachovávají.

   Jaké jsou první čtyři znaky původního textu? [6 bodů]

4. Napište vzorec pro výpočet x_{n+1}, nakreslete vysvětlující obrázek a spočtěte první tři iterace *metody sečen* při vyšetřování kořenů funkce

$$y = f(x) = x^2 - 10 \sin x.$$

   Kořen hledejte na ohraničujícím intervalu $\langle x_0, x_1 \rangle = \langle 2{,}4; 2{,}6 \rangle$. Stačí počítat na tři platné číslice. [8 bodů]

Pokračování na další straně.

5. Na jakém principu funguje algoritmizační paradigma nazývané „dynamické programování“? [2 body]

6. Zapište rovnice pro kódování a dekódování exponenciální šifry (což je například šifra RSA). [2 body]

7. Co je to třída kongruence? Zapište třídu kongruence, do níž patří všechna lichá čísla. [2 body]

8. Co je to *sblížený zlomek*? [1 bod]

9. Pravda / nepravda: Pokud iterativní metoda pro řešení nelineárních rovnic zpřesní[1] v n-té iteraci výsledek o konstantní počet bitů, říkáme, že metoda má konstantní rychlost konvergence. [2 body]

10. Jak byste charakterizovali algoritmus s paměťovou složitostí $\mathcal{O}(n^4)$? [2 body]

11. Jaká je absolutní a relativní chyba aproximace čísla $\sqrt{2}$ hodnotou 1,41? [2 body]

12. Uveďte příklad *nekorektní* numerické úlohy? [2 body]

13. Pravda / nepravda: Newtonova metoda je příkladem metody prosté iterace (angl. *fixed-point iteration scheme*). [1 bod] Jaký tvar má rovnice řešená metodou prosté iterace? [1 bod]

14. Pokud byste při numerické integraci funkce volili mezi obdélníkovým pravidlem a lichoběžníkovým pravidlem, které byste zvolili a proč? [2 body]

[1] přidá k již dosažené přesnosti výsledku

Řešení

1. Nejprve je třeba převést násobitele x z levé strany na pravou. Toho dosáhneme například použitím modulární inverze:

$$\begin{aligned}(3\cdot 3)\,x &\equiv 3\cdot 1 \pmod 4,\\ (3\cdot 2)\,x &\equiv 3\cdot 1 \pmod 5,\\ (5\cdot 2)\,x &\equiv 5\cdot 3 \pmod 9,\end{aligned}$$

a po úpravě

$$\begin{aligned}x &\equiv 3 \pmod 4,\\ x &\equiv 3 \pmod 5,\\ x &\equiv 6 \pmod 9.\end{aligned}$$

▶ Tuto soustavu řešíme klasickým algoritmem

i	a_i	M_i	N_i	n_i
1	3	1	45	4
2	3	1	36	5
3	6	5	20	9

Výsledná třída kongruence je pak dána modulem 180 a hodnotou

$$x = 3\cdot 1\cdot 45 + 3\cdot 1\cdot 36 + 6\cdot 5\cdot 20 = 135 + 108 + 600 = 843.$$

Výsledek je tedy

$$x \equiv 123 \pmod{180} \Leftrightarrow x = 123 + k\cdot 180.$$

▶ Alternativně

$$\begin{aligned}q_1 = 45 \equiv 0 \pmod{5\cdot 9} \quad &\wedge \quad q_1 = 45 \equiv 1 \pmod 4,\\ q_2 = 36 \equiv 0 \pmod{4\cdot 9} \quad &\wedge \quad q_2 = 36 \equiv 1 \pmod 5,\\ q_3 = 100 \equiv 0 \pmod{4\cdot 5} \quad &\wedge \quad q_3 = 100 \equiv 1 \pmod 9.\end{aligned}$$

Výsledná třída kongruence je pak dána modulem 180 a hodnotou

$$x = 3\cdot 45 + 3\cdot 36 + 6\cdot 100 = 135 + 108 + 600 = 843.$$

Výsledek je tedy

$$x \equiv 123 \pmod{180} \Leftrightarrow x = 123 + k\cdot 180.$$

Bodování: 1 bod za převod do upravené formy, 3 body za tabulku nebo soustavu kongruencí q_1 až q_3, 2 body za výpočet do výsledku, 1 bod za to, že výsledek zapíšou v jedné ze dvou akceptovatelných forem znázorněných výše.

2. Podle Eulerova vzorce lze součet řady

$$x = -\frac{1}{2} + \frac{1}{10} - \frac{1}{19} + \frac{1}{27} - \frac{1}{36} + \frac{1}{44} - \frac{1}{53}\ldots$$

s koeficienty

$$c_1 = -2,\ c_2 = -10,\ c_3 = -19,\ c_4 = -27,\ c_5 = -36,\ c_6 = -44,\ c_7 = -53$$

(řada má alternující znaménka a začíná kladným) zapsat jako

$$x = \cfrac{1}{-2 + \cfrac{4}{-8 + \cfrac{100}{-9 + \cfrac{361}{-8 + \cfrac{729}{-9 + \cfrac{1296}{-8 + \cfrac{1936}{-9 + \dots}}}}}}}.$$

Rekurentě spočítané sblížené zlomky jsou

$$\begin{aligned}
S_1 &= \frac{A_1}{B_1} = \frac{(-2)\cdot 0 + 1\cdot 1}{(-2)\cdot 1 + 1\cdot 0} = -\frac{1}{2} = -0{,}50000 \\
S_2 &= \frac{A_2}{B_2} = \frac{(-8)\cdot 1 + 4\cdot 0}{(-8)\cdot(-2) + 4\cdot 1} = -\frac{8}{20} = -0{,}40000 \\
S_3 &= \frac{A_3}{B_3} = \frac{(-9)\cdot(-8) + 100\cdot 1}{(-9)\cdot 20 + 100\cdot(-2)} = -\frac{172}{380} = -0{,}45263 \\
S_4 &= \frac{A_4}{B_4} = \frac{(-8)\cdot 172 + 361\cdot(-8)}{(-8)\cdot(-380) + 361\cdot 20} = -\frac{4264}{10260} = -0{,}41559 \\
S_5 &= \frac{A_5}{B_5} = \frac{(-9)\cdot(-4264) + 729\cdot 172}{(-9)\cdot 10260 + 729\cdot(-380)} = -\frac{163764}{369360} = -0{,}44337 \\
S_6 &= \frac{A_6}{B_6} = \frac{(-8)\cdot 163764 + 1296\cdot(-4264)}{(-8)\cdot(-369360) + 1296\cdot 10260} = -\frac{6836256}{16251840} = -0{,}42065 \\
S_7 &= \frac{A_7}{B_7} = \frac{(-9)\cdot(-6836256) + 1936\cdot 163764}{(-9)\cdot 16251840 + 1936\cdot(-369360)} = -\frac{378573408}{861347520} = -0{,}43951
\end{aligned}$$

3. Vzorec, který asi bude nejčastější, je

$$x_{n+1} = x_n - \frac{x_n - x_{n-1}}{f(x_n) - f(x_{n-1})} \cdot f(x_n)$$

případně si ti chytřejší pamatují

$$x_{n+1} = x_n + \frac{s_n}{1 - s_n} \cdot (x_n - x_{n-1}), \quad s_n = \frac{f(x_n)}{f(x_n)}.$$

Za použití

$$x_{n+1} = \frac{x_{n-1} f(x_n) - x_n f(x_{n-1})}{f(x_n) - f(x_{n-1})}$$

dávám jednobodovou penalizaci, protože ten vzorec je pro výpočet nevhodný a říkal jsem jim to.

Prvních šest iterací

$$y = f(x) = x^2 - 10\sin x$$

počínajících intervalem $\langle 2{,}4; 2{,}6\rangle$ je

iterace	a	b	$f(a)$	$f(b)$	c	$f(c)$
1	2,40000	2,60000	−0,99463	1,60499	2,47652	−0,03799
2	2,47652	2,40000	−0,03799	−0,99463	2,47956	0,00101
3	2,47956	2,47652	0,00101	−0,03799	2,47948	−0,00000
4	2,47948	2,47956	−0,00000	0,00101	2,47948	−0,00000
5	2,47948	2,47948	−0,00000	−0,00000	2,47948	−0,00000
6	2,47948	2,47948	−0,00000	−0,00000	2,47948	−0,00000

Bodování: 8 bodů za kompletní výpočet, 2 body za vzorec a 1 za obrázek.